

# Lateral Movement with Mimikatz

---



**Lee Allen**  
PENETRATION TESTER



# Mimikatz



# Mimikatz

Creator: Benjamin Delpy



Mimikatz is a tool used to extract plain text passwords, hashes, kerberos tickets, and PIN codes from memory. In addition Mimikatz can also be used to pass the hash, pass the ticket or create golden and silver tickets



# Mimikatz

Well-known credential dumping tool

Used for lateral movement

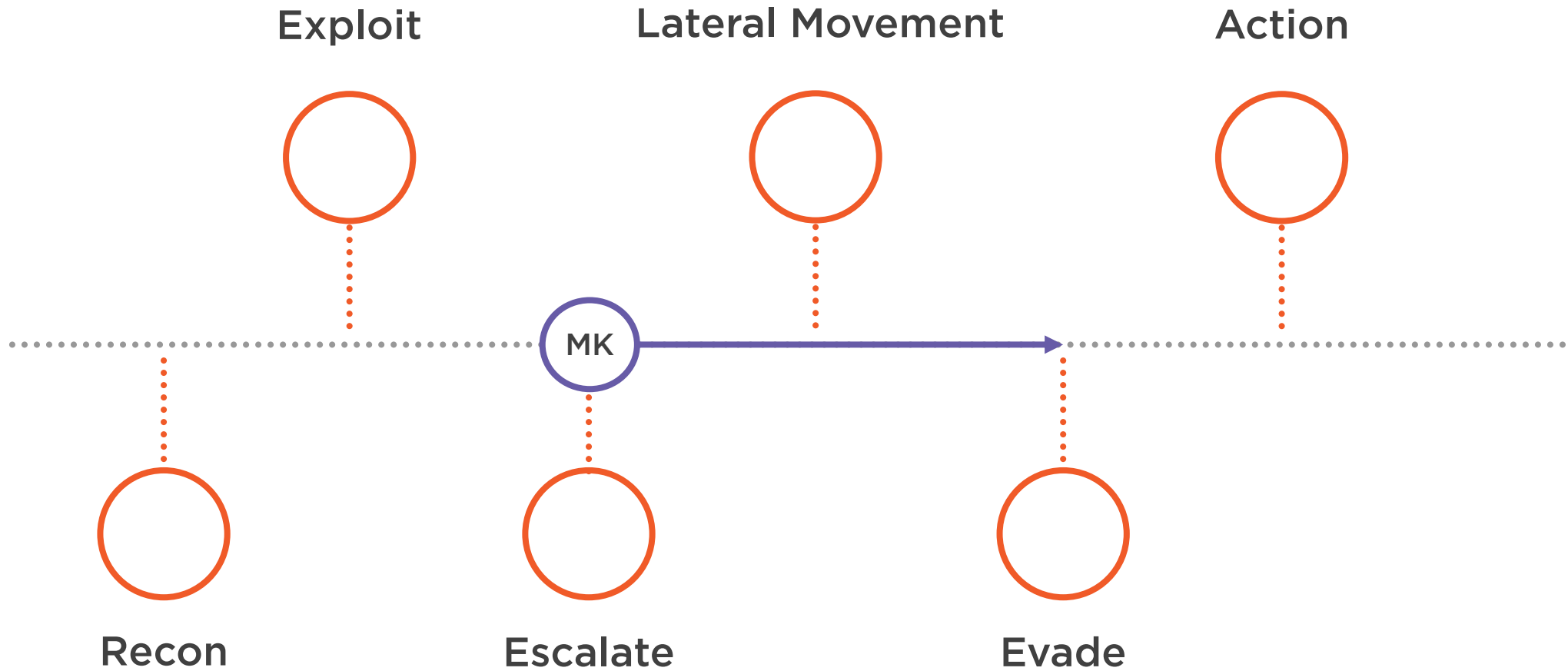
Used towards defense evasion

GitHub:

- <https://github.com/gentilkiwi/mimikatz>



# Kill Chain



# MITRE ATT&CK

## Tactics

Initial Access  
Execution  
Persistence  
Privilege Escalation  
Defense Evasion  
Credential Access  
Discovery  
Lateral Movement  
Collection  
Command & Control  
Exfiltration  
Impact



# MITRE ATT&CK

## Tactics

Initial Access

Execution

Persistence

Privilege Escalation

**Defense Evasion**

Credential Access

Discovery

**Lateral Movement**

Collection

Command & Control

Exfiltration

Impact

T1207:

DCShadow

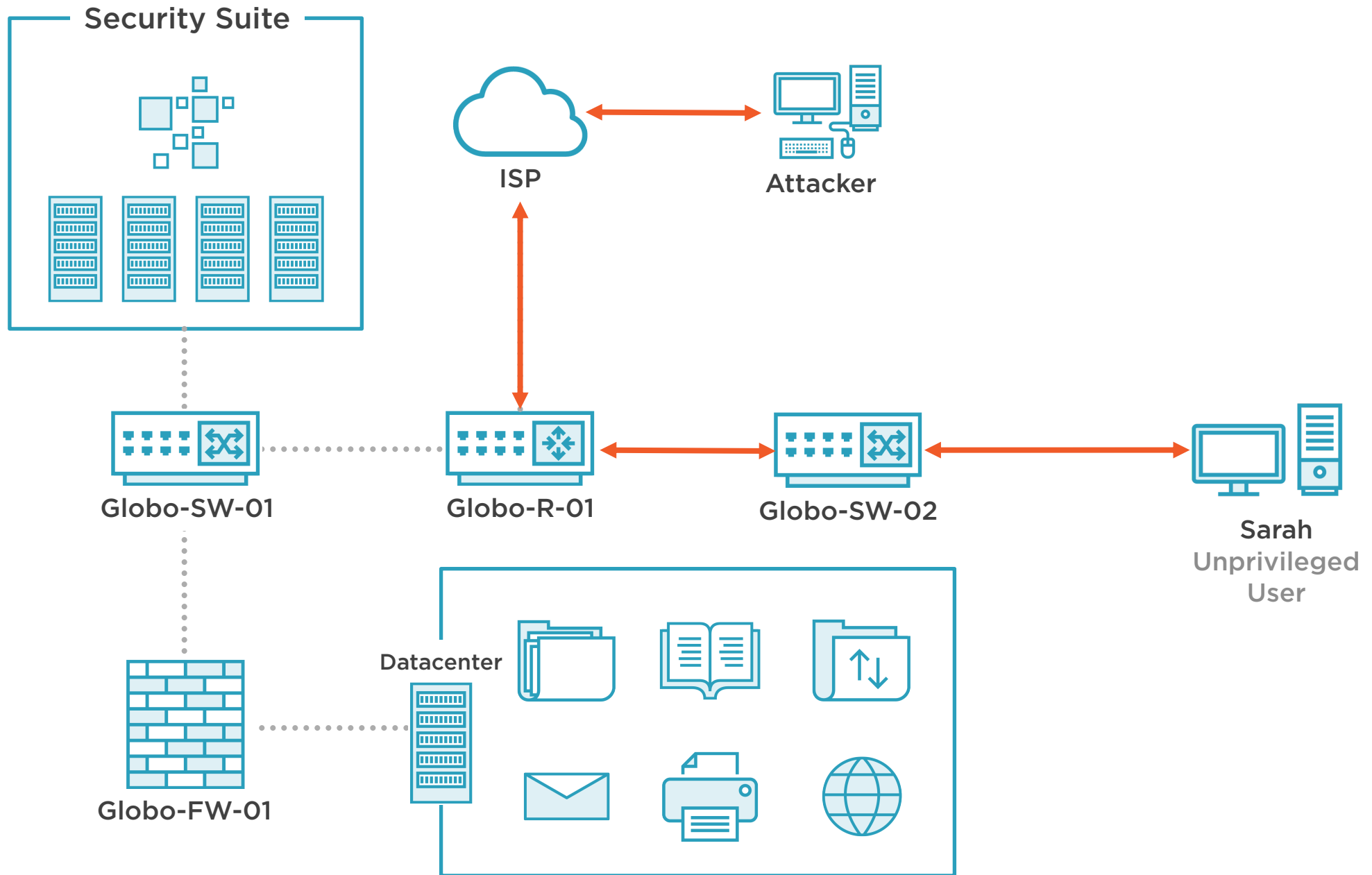
T1075:

Pass the Hash

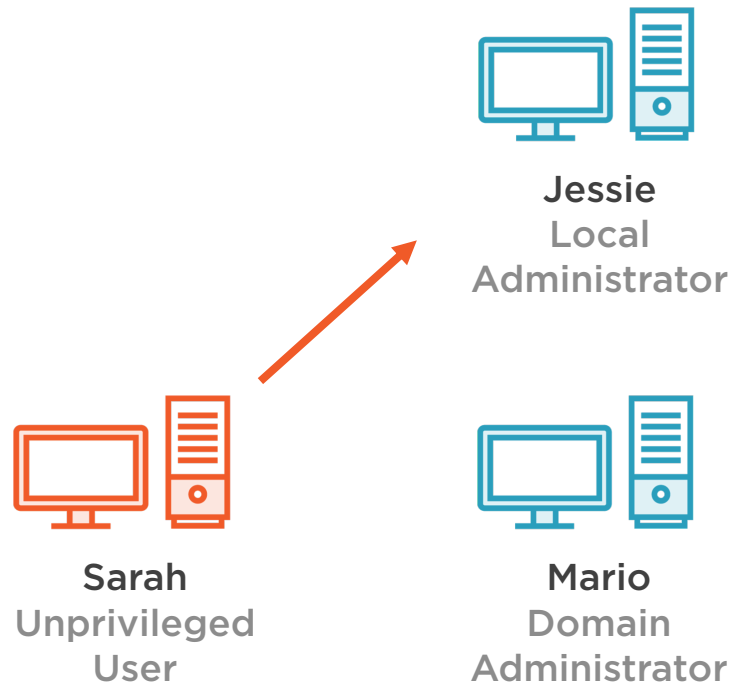
T1097:

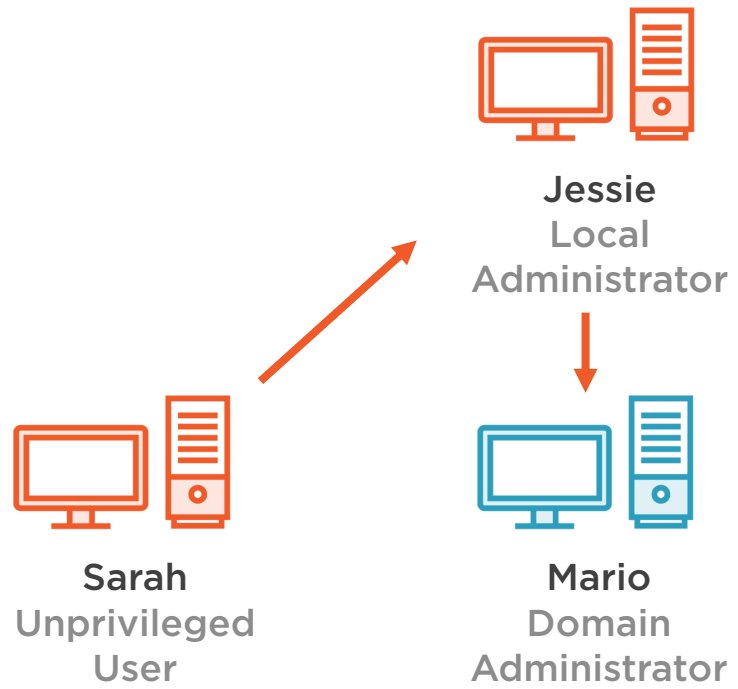
Pass the Ticket

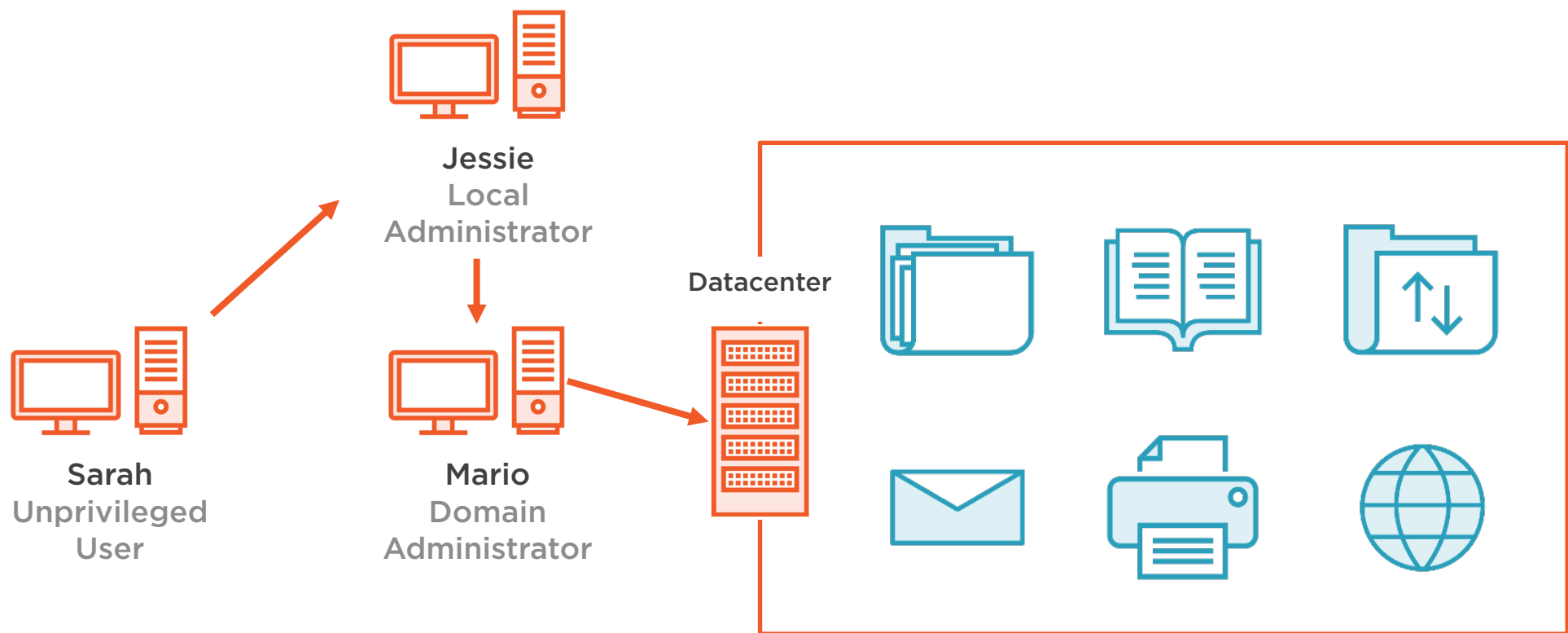












# Demo



## Using Mimikatz to Pass the Hash (PTH)



# Demo



Use Mimikatz to Pass the Ticket (PTT)



# Demo



Use Mimikatz to create Golden Tickets



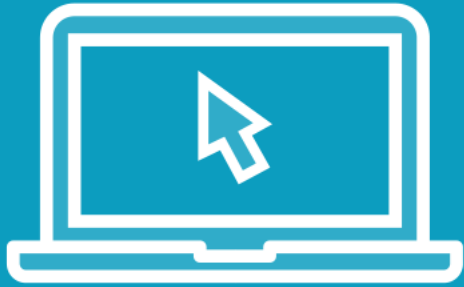
# Demo



Use Mimikatz to create Silver Tickets



# Demo



Register a rogue domain controller with  
DCShadow





# More Information

## Capabilities

Mimikatz Wiki

<https://github.com/gentilkiwi/mimikatz/wiki>

MITRE ATT&CK

<https://attack.mitre.org/software/S0002/>

Active Directory Security - Unofficial Guide to Mimikatz & Command Reference

<https://adsecurity.org/?p=2207>

## Additional Resources

Benjamin Delpy on Twitter

<https://twitter.com/gentilkiwi?lang=en>

